Installationsanleitung
Bring Your Own Device (BYOD)

für die freiwillige Nutzung privater Geräte für geschäftliche Anwendungen

Mit der folgenden Anleitung können Sie Ihre privaten Mobilgeräte auf freiwilliger Basis in das Brau Union - Unternehmensportal einbinden und somit APPs wie Workplace und MyHR auf Ihrem Mobilgerät installieren und verwenden. Allen Inhabern einer Firmen-Mailadresse steht auch Outlook und TEAMs mobil zur Verfügung

Sämtliche Screenshots können je nach Gerät und System-Version etwas abweichen und dienen als schrittweise Orientierungshilfe bei der Einbindung Ihres Gerätes.

Alle Bildschirmausschnitte in dieser Anleitung wurden mit IOS 17.4.1 erstellt.

Aufgrund von Sicherheitsrichtlinien können nur Geräte, deren Betriebssystemstand mindestens Android 10 oder iOS 14 aufweist, eingebunden werden.

Am Ende dieser Anleitung finden Sie zur Information die Richtlinien für die Verwendung privater Geräte.

Schritt-für-Schritt Anleitung

1. Unternehmensportal APP herunterladen und App öffnen

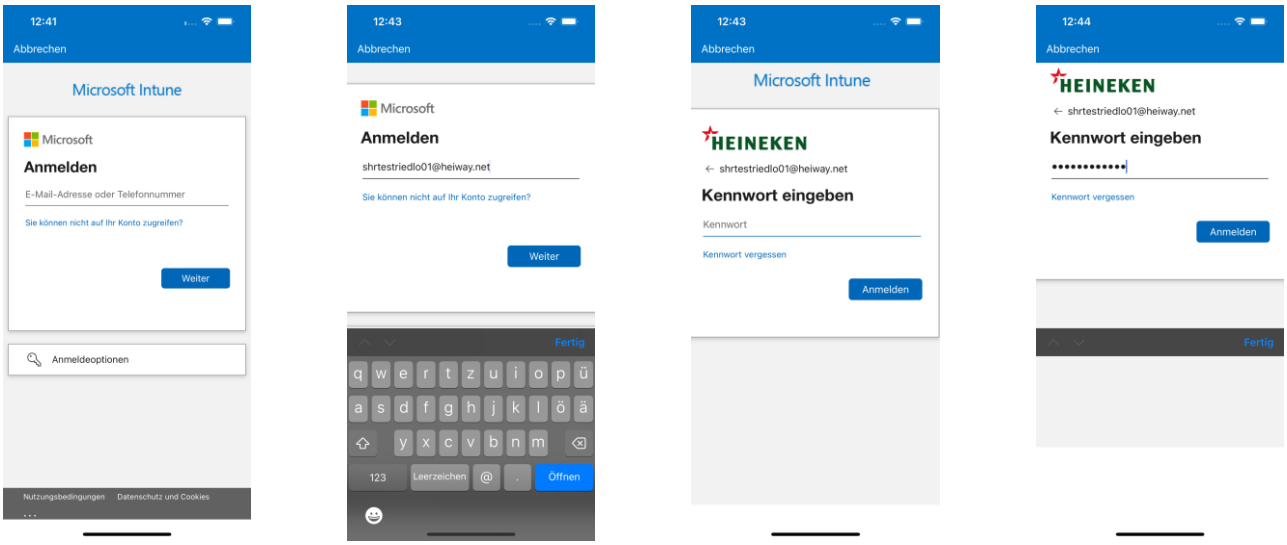
iOS App Store Google Play Store Unternehmensportal APP:

2. Heineken Nutzungsbedingungen akzeptieren

Zu Beginn der Einbindung werden Sie aufgefordert, die Heineken Richtlinie zu bestätigen. Diese Richtlinie kann ab Seite 4 im Detail nachgelesen werden.

3. Anmelden

Windows AD-Benutzer eingeben: ADUser@heiway.net (z.B.: MusteM01@heiway.net)
Danach wird Ihr Windows PC Anmeldekennwort abgefragt.



Zum Zurücksetzen des Passwortes bitte den Servicedesk kontaktieren (0732/6979-7000). Aus Sicherheitsgründen wird das Passwort nicht telefonisch übermittelt, sondern per E-Mail an den Vorgesetzten.

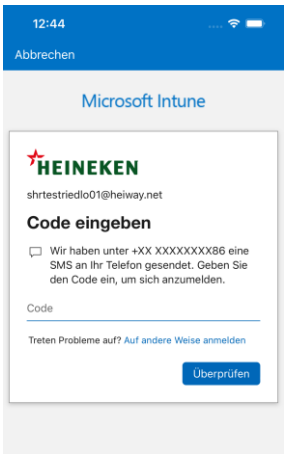
Achtung! Das neue Passwort muss sofort geändert werden. Das kann nur auf einem PC durchgeführt werden und ist nur einmalig erforderlich.
Die Länge muss mindestens 12 beliebige Zeichen betragen. Nach 365 Tagen ist es erneut zu ändern.

4. Bestätigen der Identität

Wählen Sie bei der 2 Faktor Authentifizierung bitte SMS-Authentifizierung.

Sie erhalten innerhalb weniger Sekunden eine SMS mit einem Code. Diesen bitte eingeben und auf Überprüfen tippen.

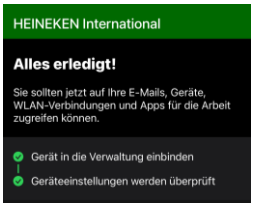
Sollte die SMS nicht ankommen, kontaktieren Sie bitte folgende Telefonnummer um Ihre hinterlegte Nummer zu überprüfen: 0732 6979 7000



5. Abschluss der Registrierung

Abschließend werden diverse Sicherheitseinstellungen konfiguriert wie z.B.: eine PIN-Vergabe, um die Firmendaten vor Zugriff unbefugter Personen zu schützen.

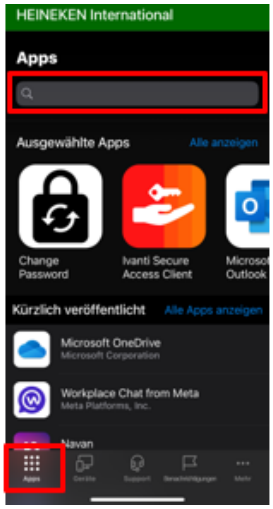
Folgen Sie den Anweisungen. Am Ende sollte die Meldung in der APP so aussehen:

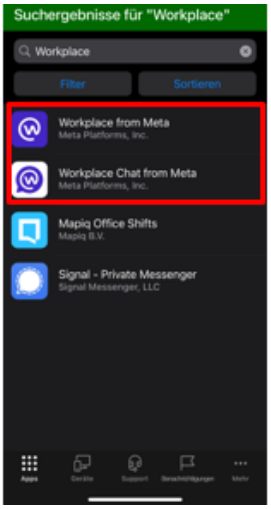


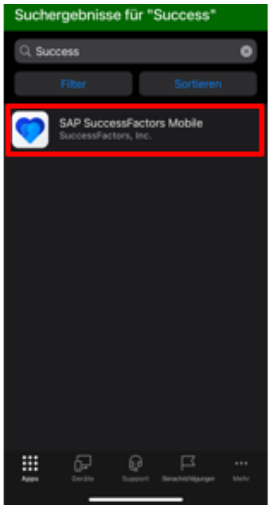
6. Installation der Unternehmens-Apps

Öffnen Sie die soeben installierte App „Unternehmensportal“. Hier können Sie sämtliche für Sie verfügbare Firmen- APPs herunterladen.

Die gewünschte App auswählen und auf „Installieren“ tippen. Nach erfolgreicher Installation können Sie die APPs auf ihrem Startbildschirm öffnen.







Workplace („Unternehmens-Facebook“):
- Anmelden mit ADUser@heiway.net + Windows AD-Kennwort
- Gruppen beitreten und Nachrichten ansehen (wie im Facebook)

M**yHR** (SuccessFactors) für Abwesenheiten und E-Learnings:
- Aktivierung mit dem Firmennamen à Heineken International eingeben
- Anmelden mit ADUser@heiway.net + Windows AD-Kennwort

Hinweis:
Wenn sie eine Brauunion-Mailadresse haben, ist die Verwendung von E-Mails und Teams ebenfalls möglich

Richtlinie

Bring Your Own Device (BYOD)

für die freiwillige Nutzung privater Geräte für geschäftliche Anwendungen

Stand April 2024

Inhalt

1. Regelungsgegenstand 6
2. Nutzungsbedingungen 6
3. Unterstützte Geräte 7
4. Supportleistungen 7
5. Kosten 8
6. Sicherheitsmaßnahmen 8
7. Beendigung der Nutzung privater Geräte 9

1. Regelungsgegenstand

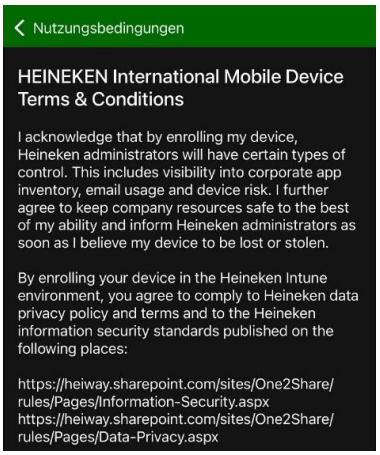
Brau Union Österreich AG (nachfolgend „BUO“) bietet Mitarbeiterinnen und Mitarbeitern (nachfolgend „MA“) die Möglichkeit, mit privaten Geräten bestimmte Unternehmensapplikationen zu nutzen. Es gelten die gleichen Zugangsberechtigungen wie für die Nutzung auf Firmen-Geräten. Diese sind an das geschäftliche Benutzerkonto (AD-User) gekoppelt.

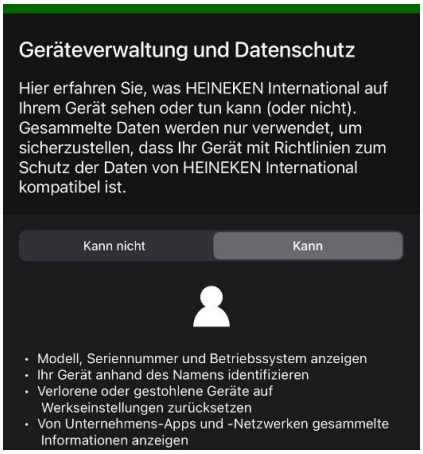
Private Geräte werden über dieselbe zentrale Plattform verwaltet wie Geräte von BUO. Dadurch kann ein sicherer Betrieb gewährleistet und Supportleistungen für die geschäftlichen Anwendungen erbracht werden.

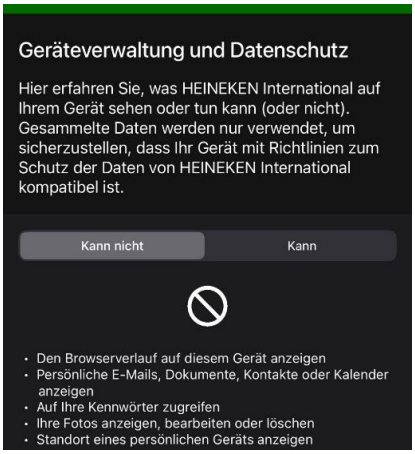
2. Nutzungsbedingungen

Der Zugriff auf Unternehmensresourcen wird über die App „Unternehmensportal“ auf dem privaten Gerät ermöglicht. Diese ist kostenlos über den App-Store des verwendeten Anbieters zu installieren. Im Zuge der Installation sind folgende Schritte durchzuführen:

- Anmeldung mit dem persönlichen AD-User (MusteM01@heiway.net) und AD PW.
- Bestätigung der Identität mit Multifaktor - Authentifizierung (z.B.: SMS)
- Vergabe eines PIN-Codes zum Entsperren des Gerätes (automatisch nach maximal 5 Minuten)
- Akzeptieren der folgenden HEINEKEN Nutzungsbedingungen* in der APP:







*Ich erkenne an, dass Heineken-Administratoren durch die Registrierung meines Geräts bestimmte Zugriffsmöglichkeiten haben. Dazu gehört der Einblick in das App-Inventar des Unternehmens, die E-Mail-Nutzung des BUO-Firmen-Mail Accounts und das Geräterisiko. Ich bin ferner damit einverstanden, die Unternehmensressourcen nach besten Kräften sicher zu halten und die Heineken-Administratoren zu informieren, sobald ich glaube, dass mein Gerät verloren gegangen, gehackt oder gestohlen wurde. Durch die Registrierung Ihres Geräts in der Heineken Intune-Umgebung erklären sich die App-Nutzer damit einverstanden, die Datenschutzrichtlinien und -bedingungen von Heineken sowie die Heineken-Informationssicherheitsstandards einzuhalten, die an den folgenden Orten veröffentlicht werden:

HEINEKEN Information Security Standard:
https://heiway.sharepoint.com/sites/One2Share/rules/Pages/information-security.aspx

HEINEKEN Data Privacy Policy:
https://heiway.sharepoint.com/sites/One2Share/rules/Pages/data-privacy.aspx

Bei der Gestattung der Nutzung privater Geräte für geschäftliche Zwecke handelt es sich um eine unverbindliche Zusage von BUO, die auch bei wiederholter und langdauernder Gewährung keinen wie immer gearteten Rechtsanspruch des jeweiligen MA für die Zukunft begründet. BUO behält sich das Recht vor, diese Richtlinie im eigenen Ermessen jederzeit (auch nur zum Teil) zu ändern oder zu widerrufen.

Der Verlust oder Diebstahl eines Gerätes muss unverzüglich via IT-Hotline gemeldet werden, um die Fernlöschung von firmenrelevanten Daten sicherzustellen. Eine Ortung des Gerätes ist in diesem Fall nicht möglich.

Folgende Handlungen sind bei der Nutzung von Unternehmensapplikationen generell untersagt:

- Speichern oder Versenden rechtswidriger Inhalte (z.B. rassistische, diskriminierende, Terror- oder pornographische Inhalte, usw.)
- Speichern oder Versenden bzw. Weitergabe geschützter Unternehmensinformationen oder illegaler Daten;
- Belästigungen Dritter
- Veröffentlichung von Firmendaten, insb. Betriebs- oder Geschäftsgeheimnisse betreffend (z.B. in sozialen Medien)

3. Unterstützte Geräte

Es werden Geräte mit dem Betriebssystem „Apple iOS“ und „Google Android“ unterstützt, die vom Hersteller des Betriebssystems mit aktuellen Sicherheitsupdates versorgt werden. Generell ist auf eine laufende Aktualisierung des Betriebssystems und der installierten Apps zu achten. Geräte mit Systemversionen, die vom Hersteller nicht mehr unterstützt werden, dürfen nicht mehr auf Unternehmensapplikationen zugreifen und werden automatisch blockiert.

Geräte, an denen vom Gerätehersteller vorgesehene Nutzungsbeschränkungen oder Sicherheitsfunktionen entfernt wurden („Jailbreak“), dürfen ebenfalls nicht für den Zugriff auf Unternehmensapplikationen genutzt werden und werden ebenfalls automatisch blockiert.

4. Supportleistungen

Der IT Service Desk unterstützt MA ausschließlich bei Anfragen im Zusammenhang mit dem Zugriff auf Unternehmensapplikationen.

Keine Unterstützung bietet der IT-Service Desk bei Problemen mit Hardware oder Betriebssystem des privaten Geräts. Für den Fall, dass ein privates Gerät nicht mehr genutzt werden kann, besteht kein Anspruch auf ein Ersatzgerät seitens BUO.

5. Kosten

Die Verwendung des privaten Gerätes für geschäftliche Zwecke erfolgt freiwillig. Zur Erledigung geschäftlicher Zwecke stehen primär IT-Systeme der BUO zur Verfügung (z.B. PCs). Zur Abwicklung des ordentlichen Geschäftsbetriebs ist der Einsatz privater Geräte nicht erforderlich. BUO trägt daher keine Kosten, die durch die Nutzung privater Geräte für geschäftliche Zwecke entstehen.

Insbesondere haben MA folgende Kosten zu tragen:

- Reparatur-, Instandsetzungs- oder Serviceleistungen
- An- oder Neubeschaffung
- Gebühre, die durch die Nutzung des privaten Geräts anfallen (insbesondere Mobilfunkgebühren oder Gebühren für private Apps und Cloud-Dienste)

BUO trägt sämtliche Kosten, die für den sicheren Zugriff und die Verwaltung privater Geräte im Zusammenhang mit der Nutzung von Unternehmensapplikationen entstehen. Das sind insbesondere:

- Lizenzkosten
- Infrastruktur für den sicheren Zugriff auf Unternehmensdaten
- Kosten für interne und externe Dienstleistungen für Geräteverwaltung und Support

6. Sicherheitsmaßnahmen

Folgende Vorkommnisse müssen der IT-Abteilung (über den Global Service Desk) umgehend gemeldet werden und haben eine Entfernung des Gerätes aus der Verwaltung zur Folge:

- Verlust
- Diebstahl
- vor Beauftragung eines Reparaturdienstes
- Ereignisse, die die Sicherheit gespeicherter Daten gefährden könnten -z.B.: Phishing Attacke.

Eine regelmäßige Sicherung der privaten Daten wird empfohlen. BUO stellt dafür keine Unterstützung zur Verfügung.

Wenn ein Gerät für mehr als 90 Tage keinen Kontakt zum Unternehmensportal aufbaut, wird es für einen Zugriff auf Unternehmensapplikationen automatisch gesperrt.

Keiner der genannten Fälle hat einen Einfluss auf private Daten und Apps.

Um einen unberechtigten Zugriff auf Unternehmensdaten zu verhindern, ist die Vergabe eines PIN-Codes erforderlich. Zusätzlich wird eine automatische Sperre des Geräts nach maximal 5 Minuten Inaktivität eingestellt. Bei zehn Versuchen, das Gerät mit einer falschen PIN zu entsperren, wird das Gerät automatisch auf Werkseinstellungen zurückgesetzt. Der PIN-Code ist ebenso vertraulich zu behandeln wie das Passwort des AD-Users.

Das Gerät ist vor der Nutzung durch Dritte (z.B.: Familienmitglieder) zu schützen, damit diese nicht auf Unternehmensdaten zugreifen können. Bei der Nutzung privater Geräte in der Öffentlichkeit muss sichergestellt werden, dass vertrauliche oder heikle Unternehmensdaten nicht von Dritten eingesehen werden können.

7. Beendigung der Nutzung privater Geräte

Der Zugriff auf Unternehmensapplikationen mit privaten Geräten wird beendet, wenn

- MA aus dem Unternehmen ausscheiden
- MA den Zugriff nicht mehr wünschen
- das Gerät verloren geht oder gestohlen wird
- die installierte Version des Betriebssystems vom Hersteller nicht mehr unterstützt wird
- eine private App eine Beeinträchtigung einer Unternehmens-App verursacht
- eine Verletzung der Richtlinien oder eine Bedrohung für die Sicherheit von Unternehmensapplikationen und Daten festgestellt wird
- BUO die Nutzung privater Geräte für geschäftliche Zwecke nicht mehr gestattet
- BUO die Nutzung der Unternehmensapplikation nicht länger gestattet